Virginia Department of Social Services

Division of Information Systems

Information Security Policy

Issued: July 15, 1992
Revised: November 18, 2003

This page intentionally left blank

Chapter 1 – Individual Use Policy

Appendices

This page intentionally left blank

Chapter 1 – Individual Use Policy

Section 1 – Introduction

The DSS (Department of Social Services) Information Security Policy is written to establish a formal policy to guide individuals in their use of DSS information and information systems. This policy is divided into several chapters, with each chapter discussing the requirements for a particular area.

Chapter 1 - Individual Use Policy. This chapter describes the general security policies of the Virginia Department of Social Services. These policies apply to everyone who uses DSS information and information systems

Chapter 2 - Special Topics. The second chapter describes the specific security requirements related to areas such as handling Internal Revenue Service and Social Security Administration information.

Chapter 3 - DSS Technical Staff. The third chapter describes the security requirements related to developing, installing, maintaining and running the DSS automated systems.

Chapter 4 - Disaster Recovery. The last chapter describes the DIS policies and procedures related to disaster recovery.

Note: Chapters 2, 3 and 4 are distributed to specific personnel as needed to perform their job function.

1.1 Purpose

The purpose of the DSS Information Security Policy is to:

- Promote information security to individuals using DSS computers and systems;
- Make each of us aware of our duty to protect DSS' information and information processing systems;
- Ensure the confidentiality, availability, and integrity of data;
- Reduce the risk of data loss by accidental or intentional modification, disclosure, or destruction; and
- Preserve the DSS's rights and remedies in the event of such a loss.

1.2 Scope

This policy applies to:

- All *Individuals* (DSS employees, employees of local welfare agencies (LWA), contractors, vendors, volunteers, work experience personnel and other persons and organizations) who have a need to use DSS related information or information processing systems;

- All information and information processing systems associated with the Department of Social Services; and
- All information and information processing systems associated with other organizations which the Department of Social Services uses, including but not limited to SSA, TAX, IRS, DMV, and VEC.

1.3 Policy Statement

DSS related information is only to be made known to and utilized by authorized individuals for authorized DSS purposes.

Electronic data processing equipment and programs developed and/or purchased by/for the Department of Social Services are the property of the Department of Social Services and may only be used for authorized purposes.

All DSS related information, data processing equipment, software and data files must be protected from accidents, misuse and unauthorized alteration. Software and data files must be documented and backed up.

Violations of this policy must be reported to the appropriate division/office/agency director and the DIS Information Security Unit. Violations of state and local laws will be reported to the appropriate law enforcement authorities. In the case of lost or missing computer equipment or software, notification must also be made to the Office of Internal Audit.

1.4 Objectives

- Ensure the integrity and protection of information and information processing systems.
- Provide for privacy of privileged or sensitive information.
- Protect information and information processing systems from the hazards of fire, water, misappropriation, misapplication, vandalism or other peril.
- Ensure the department's ability to provide services and benefits to its customers.
- Describe individual responsibilities for information security.

1.5 Individual Responsibilities and Compliance

Every *Individual* using DSS information and/or information systems is responsible for reading, understanding and complying with all of the Department of Social Services' Information Security Policies. Each person must also read, sign and abide by the Information Security Access, Inspection & Monitoring Policy (ISAIMP), see Appendix B - Forms.

When policies are violated, these violations will be brought to the attention of management for appropriate action. Depending on the severity, an employee who violates these policies may receive a Group II or Group III Standards of Conduct Offense; and prosecuting action may be undertaken if they knowingly and intentionally violate any local, state or federal laws, or use any DSS related information, information processing systems or equipment for fraudulent, extortive or destructive purposes

Exceptions to this policy must be clearly documented, reviewed and approved by DSS's Division of Information System's (DIS) Information Security Unit. [1]

A summary of all security related issues can be found in Appendix C.

1.6 Authority

The policies described in this document are based on requirements found in the following codes, policies, regulations, laws, standards and guidelines:

- Code of Virginia, Chapter 52 (see Appendix B)
- COV ITRM Standard SEC2001-01.1, (12/7/2001), Information Technology Security Standard
- COV ITRM Guideline SEC2000-01.1, (12/7/2001), Information Technology Security Guideline
- COV ITRM Guideline SEC2001-01.1, (2/27/2001), Internet Privacy Guidelines
- TANIF Manual 103.1 (1/20/97), Purpose of Safeguarding of Information and Scope of Regulations
- VDSS/DCSE Manual, Chapter 2 (11/1/96), Confidentiality/Information Release
- USDA/FNS 7 CFR .72.1(c), 272.1(d), Disclosure of Information
- HHS 45 CFR 303.21 and 45 CFR 303.105
- IRS Revenue Procedure Section 6103 (L)(7)(b), Disclosure of Information to Federal, State, and Local Agencies
- Public Law 100-235, Computer Security Act of 1987
- Virginia Social Service Laws 63.2 (2002)
- Virginia State Library and Archives, Records Retention and Disposition Schedules (RM-2) (7/94)

Section 2 – Responsibility

2.1 Policy

Each division, office, region, district and local agency must have an effective security administration function in place.

2.2 Background

For an information security policy to be effective, someone in each division, office, region, district and local agency should be assigned the responsibility for developing security procedures and administering the security program in their unit. The individual selected should be cognizant of data processing and information security fundamentals and possess sufficient abilities to develop, implement and enforce information security procedures.

2.3 Requirements and Guidelines

Each division, office, district, region and local agency must designate a security officer and backup security officer whose responsibility is to ensure compliance with the DSS Information Security Policies and Guidelines. They must also develop, implement and maintain local information security procedures. These procedures should ensure compliance of the DSS Information Security Policies Requirements and Guidelines described in this document.

2.4 Responsibility

This section describes the security responsibilities for agencies, offices and groups within DSS.

2.4.1 Executive Management

The Commissioner, through the Information Security Unit, is responsible for assuring that Information Security Policies are developed and distributed to all DSS employees, LWAs, contractors, vendors and other persons and organizations who have a need to use DSS related information and information processing systems. The Commissioner is responsible for final interpretation of this policy.

2.4.2 Division/Office/District/Regional Management

Division, Office, District and Regional directors are responsible for appointing security officers and backup security officers; developing, implementing, and enforcing procedures within their units which ensure compliance with the Information Security Policies and Guidelines. Directors are also responsible for

reporting violations or suspected violations of the Information Security Policy to the DSS Information Security Unit.

Each division, office, district, and region should ensure that all of their users of information and information systems are made aware of and receive continuing training on security requirements.

2.4.3 Local Agencies

Local agency directors are responsible for appointing security officers and backup security officers; developing, implementing, and enforcing procedures within their agencies which ensures compliance with the Information Security Policies and Guidelines. Local agency directors are responsible for reporting violations or suspected violations of the Information Security Policy to the DSS Information Security Unit.

Local agencies should ensure that all of their users of information and information systems are made aware of and receive continuing training on security requirements.

2.4.4 Security Officers

Division, Office, District, Regional and Local Agency security officers are responsible for assisting employees in obtaining access to information processing resources as needed to allow authorized employees to accomplish their normal daily functions.

The primary duties of the security officer include:

- Policies. Assure that all individuals are aware of and are adhering to current DSS information security policies.
- Security Training. Provide necessary security training to the individuals as policy changes occur and to reinforce existing policies. Keep individuals up-to-date with current security issues and threats.
- Security Incidents. Notify the DSS Information Security Unit of all security incidents that may compromise system security. Provide a summary of corrective action taken or recommendations for eliminating the cause of the incident. Assist the DSS Information Security Unit with resolving security incidents that affect their area (e.g. resolving virus problems on infected PCs).
- System Access. Provides administrative support for individual access to systems. This support includes assigning a userID to new individuals, resetting expired or suspended passwords, and removing user access privileges when no longer needed.
- Investigation. Investigate possible system abuse in their area.

2.4.5 System Administrators

The DSS system administrators shall monitor performance, provide problem determination, production support, and perform system back-ups. Security responsibilities can include, but may not be limited to, ensuring that:

- Installed Software. Only authorized and approved software is installed on the system.
- Security Procedures. Approved security procedures are followed, and that the system is operated, used, and maintained in accordance with polices set forth in the DSS Information Security Policy and the individual policies listed in section 1.6 Authority of this manual.
- System Monitoring. System reviews are performed to identify unusual activity. Institute protective or corrective measures if a security problem exists.
- Security Controls. Systems are installed and operated using no less than the security controls provided by the vendor and using any security controls specified in the department's applicable security policies.
- Software Changes. The DSS Information Security Unit is notified of changes to software that might impact system security features before installation of those changes.
- Software Licensing. Procedures for software license validation and virus testing, where applicable, have been followed.
- Audit Trail. Audit trails are regularly reviewed. Develop an auditing procedure to assure that all security-related audit records will be retained in usable form for a period of 1 year.
- Security Incidents. Report security incidents or violations to the DSS Information Security Unit, with a recommendation for eliminating the cause of the incident.

2.4.6 Network and Firewall Administrators

Ensure that approved security procedures are followed, and that the networks are operated, used, and maintained in accordance with the DSS Information Security Policy and the individual policies listed in section 1.6 Authority of this manual. In addition, security responsibilities can include, but may not be limited to:

- Security Review. Review all requirements documents, configurations changes, and system changes to ensure that network security is not degraded.
- Network Policy. Develop, implement, manage and plan policy; provide guidance and assistance in network security matters.

- Contingency Planning. Ensure proper contingency planning and backup are implemented for each network.
- Security Measures. Ensure security measures and procedures used at network nodes fully support the security integrity of the network. Manage the overall security operation of Network 2000. (see Section 7 – Networks)
- Monitoring. Monitor network activities in their areas to ensure security procedures are being followed.
- Audit Trails. Review the contents of network audit trails daily for unauthorized use.
- Security Incidents. Report all network security violations and security incidents to the DSS Information Security Unit manager.
- Security Audits. Conduct network security audits, as necessary, at central and remote locations to ensure the security and integrity of Network 2000.

2.4.7 DSS Information Security Unit

This unit is responsible for providing technical information, security assistance, and for fostering and overseeing the department's information security program. Specific responsibilities will include but are not limited to:

- Technical Assistance. Providing technical assistance to divisions, offices, districts, regions and local agencies in developing, implementing and administering their security programs and procedures;
- Security Policies. Developing, maintaining and disseminating Information Security Polices and Guidelines. Ensuring their uniform interpretation and implementation throughout DSS;
- Security Policy Compliance. Ensuring that periodic reviews of the security and protection of DSS information and information systems are done to ensure compliance with the Information Security Policy;
- Risk Analysis. Performing business impact analysis and risk assessment studies for DSS' information technology systems;
- Disaster Recovery. Developing, maintaining and disseminating a disaster recovery plan for the department. Performing an annual disaster recovery test;
- Security Awareness and Training. Training individuals using information systems on proper methods of securing and controlling those resources. Promoting information security awareness and providing training; and
- Security Incidents. Reviewing information systems security incident reports. For those incidents that reveal a problem, coordinate corrective action to prevent a similar occurrence. Investigate alleged security breaches.

Section 3 – Data Sensitivity/Protection

3.1 Policy

All DSS employees, employees of local welfare agencies (LWA), contractors, vendors, volunteers, work experience personnel and other persons and organizations who have a need to use sensitive or confidential DSS related information must protect it from misuse and unauthorized disclosure.

3.2 Background

The Department of Social Services handles sensitive information that requires special handling to maintain confidentiality and availability. Our clients provide us with information that is extremely personal and sensitive, and it's our responsibility to protect it. We also work with Privacy Act information and IRS information, and by law are required to safeguard personal data such as a "social security number", "date of birth", and "name".

To help quantify our data sensitivity and protection requirements, DSS conducts and periodically updates a business impact analysis for its information processing systems. This analysis evaluates the criticality (e.g. the length of time that DSS can continue to function without the application) and confidentiality of each system, and uses the results to determine the overall sensitivity of each application and the information that the application processed.

The table on the next page shows the sensitivity score and sensitivity level for each DSS application.

DSS Application Sensitivity Table

Application Acronym	Sensitivity Score	Sensitivity Level	Application Acronym	Sensitivity Score	Sensitivity Level
ADAPT	20	High	NAPS	12	Medium
AATS	11	Medium	OASIS	17	High
APCO	15	High	PAAPPTRK	11	Medium
APECS	17	High	PDS	12	Medium
BF-12	9	Medium	QCS	11	Medium
CRC	11	Medium	R&R25	5	Low
CRF	15	High	RMS	11	Medium
E&E	6	Low	SDX	13	Medium
EAP	15	High	Service Fee Dir	11	Medium
ESP	15	High	SRATRK	12	Medium
FAAS	17	High	SSAMS	6	Low
FARS	11	Medium	SUPE	17	High
FSAPPTRK	17	High	SVES	17	High
FSCLMS	13	Medium	TOP	11	Medium
FSET	7	Medium	TRNG	11	Medium
HRM Tracking	13	Medium	TUMS	12	Medium
IDC	13	Medium	VAAOS-Licensing	9	Medium
IEVS	11	Medium	VACIS A/P/P	20	High
Job Queue	15	High	VACIS Generic	17	High
LASER	11	Medium	VACIS Resources	15	High
Learnfare	6	Low	VACIS-AFDC	17	High
LETS	15	High	VACIS-FS	17	High
MEDPEND	11	Medium	VACIS-Services	17	High
MSI/MSU	17	High	VNIS	6	Low

Section 4 – Information

4.1 Policy

DSS related information is only to be made known to and used by authorized individuals for authorized purposes and must be protected against unauthorized use, theft, vandalism, or other peril.

4.2 Background

DSS related information is regarded as an asset by the department. As such, it is to be afforded a level of control and protection commensurate with its value and sensitivity to the customer, department, division, office, agency and individual.

4.3 Requirements and Guidelines

4.3.1 DSS

All information, regardless of the medium, that contains client specific information is considered confidential and must be restricted to personnel who are authorized to use the information.

A. Information Use and Disclosure. Use and disclosure of client, financial and statistical information shall only be made by individuals who have the authority to do so.

B. Authorized Use. Information provided by internal or external sources can only be made available to personnel who have been identified by the owner of the data as having a need to know.

C. Confidential Information. Confidential information must be protected from unauthorized access at all times.

D. Disposal. Confidential information should be properly disposed of (i.e., shred, pulp, or burn; but not tossed in the trash) when it has reached its retention date or when the owner of the data determines it is no longer needed. The retention of financial, statistical and client information must comply with the Virginia State Library and Archives, Record Retention and Disposition Schedule (RM-2).

4.3.2 The Virginia Data Collection and Dissemination Practices Act, (*formerly known as the Virginia Privacy Act*):

A. § 2.2-3800.C

1. There shall be no personal information system whose existence is secret.
2. Information shall not be collected unless the need for it has been clearly established in advance.
3. Information shall be appropriate and relevant to the purpose for which it has been collected.
4. Information shall not be obtained by fraudulent or unfair means.
5. Information shall not be used unless it is accurate and current.
6. There shall be a prescribed procedure for an individual to learn the purpose for which information has been recorded and particulars about its use and dissemination.
7. There shall be a clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information.
8. Any agency holding personal information shall assure its reliability and take precautions to prevent its misuse.
9. There shall be a clearly prescribed procedure to prevent personal information collected for one purpose from being used for another purpose.
10. The Commonwealth or any agency or political subdivision thereof shall not collect personal information except as explicitly or implicitly authorized by law.

B. § 2.2-3803.A

1. Collect, maintain, use, and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated, or necessary to accomplish a proper purpose of the agency;
2. Collect information to the greatest extent feasible from the data subject directly;
3. Establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls;

4. Maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to ensure fairness in determinations relating to a data subject;

5. Make no dissemination to another system without (i) specifying requirements for security and usage including limitations on access thereto, and (ii) receiving reasonable assurances that those requirements and limitations will be observed. This subdivision shall not apply, however, to a dissemination made by an agency to an agency in another state, district or territory of the United States where the personal information is requested by the agency of such other state, district or territory in connection with the application of the data subject therein for a service, privilege or right under the laws thereof, nor shall this apply to information transmitted to family advocacy representatives of the United States Armed Forces in accordance with subsection N of § 63.2-1503;

6. Maintain a list of all persons or organizations having regular access to personal information in the information system;

7. Maintain for a period of three years or until such time as the personal information is purged, whichever is shorter, a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority but excluding access by the personnel of the agency wherein data is put to service for the purpose for which it is obtained;

8. Take affirmative action to establish rules of conduct and inform each person involved in the design, development, operation, or maintenance of the system, or the collection or use of any personal information contained therein, about all the requirements of this chapter, the rules and procedures, including penalties for noncompliance, of the agency designed to assure compliance with such requirements;

9. Establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security; and

10. Collect no personal information concerning the political or religious beliefs, affiliations, and activities of data subjects that is maintained, used or disseminated in or by any information system operated by any agency unless authorized explicitly by statute or ordinance.

4.4 Laws and Consequences

4.4.1 Privacy Act of 1974. Provides that unauthorized access to or disclosure of personal information in any manner to any person or agency not entitled to

receive it is a misdemeanor. Violators are subject to a fine of not more than $5,000.

4.4.2 Internal Revenue Code (IRC 7213 & 7431). Provides that unauthorized disclosure of any information provided by the IRS is a felony punishable by a fine not to exceed $5,000 or imprisonment for not more than 5 years or both. Taxpayers may also bring civil action for damages sustained by the plaintiff as a result of such unauthorized disclosure.

4.4.3 Fair Credit Reporting Act. Under this law, obtaining information under false pretenses or unauthorized disclosure of information is punishable by a fine of up to $5,000 or one year's imprisonment or both. Consumers may also bring civil suit for damages they sustain, and the court may also award a civil penalty of up to $1,000 for knowing and willful violations.

4.4.4 Freedom of Information Act. This act opens agency records to the public but requires the agency to ensure that policies and procedures are in place to review requests for information and deny release of protected and sensitive information. It provides for a civil penalty of up to $1,000 for knowing and willful violations.

4.4.6 Virginia Security Acts.

- Virginia Data Collection and Dissemination Practices Act (2.2-3800)
- Virginia Public Records Act (42.1-76)
- Computer Crimes Act (152.1)

4.5 DSS Penalties for Security Violations

4.5.1 Any employee who violates the Information Security Policy may be subject to a Standards of Conduct.

4.5.2 Violations by others may result in actions which Executive Management deems appropriate.

4.5.3 DSS cooperates with law enforcement agencies in the investigation and prosecution of any violations of these laws.

Note: Please refer back to section 1.5 Compliance for additional information.

Section 5 – Security Incident Reporting

5.1 Policy

Each person who uses DSS related information or information processing system is responsible for reporting security incidents, violations and suspected violations of the Information Security Policy.

5.2 Incident Identification

A common question is, "What is a computer security incident and who should I tell if I know about one?" A security incident covers a wide range of mishaps from a suspended password, to computer viruses, to a natural disaster. Each incident has a different degree of severity and depending on the severity a different way to report the incident.

To assist you with determining the severity of an incident and the proper way to handle the reporting, please refer to the table below. It separates incidents into 5 types, and gives the name of the type, examples of the incidents, and the proper way to report it. Please note: the table gives representative examples of each incident type, but the examples should not be considered all-inclusive.

Incident Type	Examples	Notify
Type 1 Operationally resolved security issues	- Suspended/expired passwords - Removal of Computer Games on PC - Updating virus software or definition files - Removing a virus from a PC - PC does not boot - Your application (e.g. ADAPT or APECS) is not working properly - You cannot access a system or a file	Report these incidents to the help desk.
Type 2 Fraud/Felony/ Deception/Abuse	- Unauthorized used of userID & password - Gaining access to restricted Internet sites - Misusing DSS equipment - Improperly accessing or disclosing confidential information - Data browsing, i.e. snooping or probing data not directly related to your job - Use of DSS equipment/facilities for illegal or wrongful purposes - Illegal copying of software/manuals/other materials - Lost or stolen PCs and software*	Report these incidents to your local management and the DSS Information Security Unit. * This must also be reported to the DSS Director of General Services and Internal Audit.
Type 3 Electronic Intrusion of Systems	- Computer viruses - Port scanning - Decrypting system or individual passwords - Intentional attempts to crash systems - Use of systems or networks to gain unauthorized access	Report these incidents to your local management and the DSS Information Security Unit.

Incident Type	Examples	Notify
Type 3 - Continued	- Using DSS systems to attack outside systems - Denial of Service attacks - Spam and chain letters	
Type 4 Unauthorized Entry of Secured Areas	- Visitors without access badges - Employee without access badges - Unauthorized or unescorted personnel in secured areas. - Break-ins	Report these incidents to your local management and/or the building security.
Type 5 Catastrophic Disasters	- Fire - Bomb threats - Hostage situations - Floods - Destruction of Property	Report these incidents to your local management, the DSS Director of General Services and the appropriate public service departments (Fire, Police, Ambulance, etc.)

Note: For additional information relating to DSS' Policy for the loss of assets, please refer to the Practices and Procedures for the Physical Security of the Theater Row Building.

5.3 Goals

If a security incident places an employee in a situation of imminent personal danger, the employee's safety is the primary concern. Once personal safety is guaranteed, the goals for handling a security incident include:

- Protection of DSS assets,
- Containment of damage,
- Data integrity,
- Data recovery,
- Restoration of service,
- Determination of the method of electronic or physical security intrusion, and
- Identification of the Intruder. [1]

5.4 Benefits

The primary benefits of a security incident program are the containment and repair of damage from incidents, and the prevention of future damage. A secondary benefit is the collection of statistics on the numbers/types of incidents, which can be used to identify and reduce future threats, and target areas for additional training. [2]

Section 6 – Security Awareness & Training

6.1 Policy

DSS shall provide training in security awareness and accepted computer security practices to all employees [DSS employees, employees of LWA, contractors, vendors, volunteers, work experience personnel] involved in the management, use, or operations of any DSS systems or applications. This training will occur for each employee upon initial hiring and prior to his or her access to any DSS system. Employees will receive periodic training to reinforce policies and to communicate new policies as required.

When an application requires specialized training, for example handling IRS information, this training will be provided on an as-needed basis for the employees involved.

6.2 Background

The DSS Information Security Unit will provide security awareness and training classes, as required, to keep DSS employees aware of their security responsibilities. DSS Information Security Unit will also provide training to security officers, so the security officers can in turn keep their employees current with changing security policies and issues.

6.3 Current Training methods

The DSS Information Security Unit has developed several methods of accomplishing its security awareness and training objectives.

- New Employee Orientation. Presenting security training to all new employees during the New Employee Orientation sessions given by the Division of Human Resource Management.
- Information Security Policy. Supplying each employee with a copy of the *Virginia Department of Social Services – Information Security Policy*.
- ISAIMP Form. Require each person using the system (employee, contractor, volunteer, etc.) to read and sign an annual ISAIMP (*Information Security Access, Inspection & Monitoring Policy*) form.
- Security Officer Training. Providing security officers with trainings sessions on policy changes and current issues so the officers can provide training to the staff in their office.
- E-mails, Broadcasts and Newsletters. Informing individuals of security concerns, issues and warnings using various electronic communication formats such as direct e-mails, local agency broadcast messages, and the *DSS Security Newsletter*.

Section 7 – Networks

DSS provides a number of network services for individuals. These services include:

- DSS Internal Website. The DSS website, referred to as *Localagency*, is part of our internal, private network and provides information to LWAs, divisions, offices, districts, regional management and the central office staff.
- DSS Public Website. As the name implies, this site is accessible by the public. The website address is http://www.dss.state.va.us/ and it gives information about DSS' programs and services.
- E-mail. E-mail allows you to send electronic mail to people within DSS and also others connected to the Internet.
- Internet. Access to the Internet permits you to do research, upload and download information, participate in chat room discussions, and the list goes on. New features and abilities are added daily.
- Network 2000. Network 2000 is DSS' intranet. It is an internal, private network for the exclusive use of DSS and its staff. The key feature of Network 2000 is it allows secure communication for sensitive and confidential information between LWAs, divisions, offices, districts, regional management and the central office.
- Network Drives. Network drive access is available to central office staff. It provides individuals with additional storage, centralized backups of information, and the ability for a number of people to have access to the same document or file.
- Remote Access. Remote access is the ability to dial-in to DSS servers from a remote location using a modem. This service is limited to DSS state staff that, by the nature of their job, are required to work remotely from home or while traveling.

7.1 Network Security Overview

DSS's network services all share some of the same basic security requirements. This section will discuss those common requirements. The subsequent sections will discuss specific security issues as they relate to each network service.

7.1.1 Policy

When using DSS network services, your first concerns should be security and maintaining confidentiality. You can be held accountable for any breaches in security or confidentiality as a result of your activities on the network. While on the network, all existing department policies will apply to your conduct as it relates to:

- Intellectual property protection (including: books, movies, music, computer programs, digital images, audio or video files and other copyrighted works)

- Privacy
- Misuse of resources
- Sexual harassment
- Data security
- Confidentiality

You are also responsible for reading and complying with the Code of Virginia, Chapter 52, Restrictions on State Employee Access to Information Infrastructure, (see Appendix B). You need to be aware of the following policies when using the network:

- Behavior. You must conduct yourself honestly and appropriately when using it;
- Business Tool. The network is a business tool to be used for department-related activities;
- DSS Image. Individuals must maintain the clarity, consistency and integrity of DSS's image and posture.
- Negative Publicity. You should protect both DSS and yourself from negative publicity and legal liabilities;
- Proper Identification. You must identify yourself accurately and completely when using e-mail and the Internet, e.g. chats and newsgroups; and
- Treatment of Others. Individuals must respect the copyrights, software licensing rules, property rights and privacy of others.

7.1.2 Requirements and Guidelines

The following guidelines should be remembered as you use the DSS networks:

- Anti-virus Software. Downloading files without department-sponsored Anti-virus software being actively running is not permitted.
- File Inspections. The department reserves the right to inspect any and all files stored in any area of the DSS network or on any device connected to the network, to ensure compliance with policy.
- Illegal Activities. Using DSS resources to knowingly violate laws and regulations or conduct illegal activity is grounds for Standards of Conduct.
- Monitoring. DSS has systems in place that monitor network and e-mail usage. When you use any of DSS' network services, you should have no expectation of privacy. Specific activities are traceable to the Commonwealth of Virginia, DSS, and the individual. Managers will review Internet activity and analyze usage patterns.

- Sexually Explicit Material. Displaying, archiving, storing, distributing, transmitting or recording any kind of sexually explicit image or document violates our policy on sexual harassment.
- Uploading/Downloading. Uploading, downloading, modifying or removing files on any node in the network, for which such action is not authorized, is forbidden. Only the manager responsible for the data or software may authorize it to be uploaded.

7.1.3 Malicious Acts.

DSS prohibits *individuals* from performing malicious acts on its networks and computer systems. The following list gives examples of forbidden acts, but this list should not be viewed as all-inclusive:

- Data Browsing. The use of DSS systems and/or networks for purposes of snooping, probing, or otherwise connecting to a node or nodes in a manner which is deemed not to be of an authorized nature;
- Decrypting Passwords. Decrypting system passwords or the passwords of other *individuals*;
- Disabling Security Features. Any attempt to disable, defeat or circumvent any security feature.
- Disabling Systems. Knowingly disabling, overloading, or intentional attempts to "crash" any computer system, network or programs;
- Hacking. Use of DSS systems and/or networks in attempts to gain unauthorized access to other computers, systems, or networks;
- Improper Use of Facilities. The use of DSS facilities and/or services for illegal, wrongful or commercial purposes;
- Malicious Code. Propagating or the willful introduction of a virus, worm, Trojan horse, or trap-door program code, or other disruptive/destructive programs into the department's network or into external networks; and
- Pirating Software. Violating copyright laws, illegal copying or pirating software, data, etc.

Malicious activity is a serious offense and can be grounds for a Standards of Conduct.

7.2 Electronic Mail (E-Mail)

7.2.1 Policy

All information pertaining to the department, its clients and others who do business with the department using e-mail, must be sent by a secure means.

7.2.2 Background

Department and local agency staff are encouraged to use e-mail for transmitting department related business messages. E-mail that is transmitted over Network 2000 (DSS' intranet) is done so on dedicated lines; therefore, these transmissions are secure because they go through DSS servers. E-mail sent over the Internet is not secure; it passes through unsecured servers managed by network administrators out of DSS' control.

7.2.3 Requirements

Only department-sponsored e-mail systems and networks (Network 2000) may be used to transmit information pertaining to the department, its clients and others who do business with the department. Only authorized individuals may send this information.

The use of free instant messaging systems, such as those provided by AOL, MSN, YAHOO, etc. are not permitted on DSS-provided computers.

7.2.4 E-mail Characteristics

E-mail is an extremely valuable and powerful tool used by DSS for its day-to-day business. However, some of the features that make it so useful, may work against you if you are not familiar with some of e-mail's basic characteristics.

- Distribution and Life Span. Once sent, you have no control over who reads your e-mail and how long it is kept. It can be intercepted en route, or the recipient can show it and/or forward it to others. Your e-mail can also be saved by anyone receiving it, and it can reappear at some future date. Remember, there is no expiration period for a statement made in haste or for an inappropriate comment.
- Illusion of Privacy. Never assume that your e-mail is private or confidential. Your e-mail can be intercepted at any point between you and your recipient. Think of e-mail as you would a post card sent through regular mail, where anyone who handles it can read the message.
- Inadvertent Disclosure. Because of its speed and the design of on-line address books, is it easy to mistakenly click on a wrong e-mail address. Always

double check the **TO:** and **CC:** sections of your e-mail header to make sure you are sending it to the appropriate people. By this simple step you may avoid sending confidential information to the wrong person.

- Irretrievable. Once e-mail is sent, it cannot be retrieved. Make sure you have thought out your message before you send it. Remember to never send e-mail in anger or haste.

7.2.5 E-mail Guidelines

When using DSS's e-mail system, please remember the following guidelines:

- Chain Letters. Chain letters should not be sent over the e-mail system.
- Dangerous Attachments. E-mail attachments have become a common method of delivering viruses or Trojan Horses. When used by hackers, these attachments are often a program or executable script. If you receive suspicious e-mail attachment and you cannot verify both the identity of sender and the program's purpose, delete it. The following is a list of some of the dangerous e-mail attachment extensions to watch for:

  exe - program files
  com - program files
  bas - Basic
  vbs - Visual Basic
  js - Java scripts
  url - Internet link
  isn - Internet link
  lnk - shortcut to files
  pif - shortcut to files

  You can greatly reduce your risk of catching a virus by watching for suspicious e-mail messages and by checking extensions before opening attachments.

  Remember, "If in doubt - delete it!"

- Encryption. Any e-mail containing confidential information pertaining to the DSS, its clients and others who do business with DSS, which is sent across the Internet, must be encrypted.
- Instant Messaging. The use of instant messaging is growing in popularity. With this growth has come increased activity on the part of hackers and vandals who exploit weaknesses in these systems. Attackers have been able to install and execute their programs on target machines. They have also been successful in implanting destructive self-propagating worms that could exploit any number of weaknesses in a PC. These worms may not be detectable by anti-virus software. As a result, the use of free instant messaging systems,

such as those provided by AOL, MSN, YAHOO, etc. are not permitted on DSS-provided computers.

- Large Attachments. E-mails that have large attachments are communications-intensive operations. If you need to send a large attachment (one to three megabytes), try to send it early morning or late afternoon. If you need to send an attachment greater than 3 megabytes, it should be put on a CD and mailed.
- Mass Mailings – DSS. If your DSS duties require that you send mass mailings, schedule these activities for off-peak times. Generally off-peak times are early in the morning or late in the day, but check with the DSS Information Security Unit if you have questions.
- Mass Mailings – Personal. Mass mailings for personal use are not allowed on DSS' networks and equipment.
- Personal Use. The department permits incidental use of e-mail for personal use; however, extensive or recurring personal use is prohibited. If you are unsure of what extensive or recurring personal use is, ask your supervisor for clarification.
- Proper Identification. You must identify yourself honestly, accurately and completely when using e-mail.
- Retention. Any e-mail remaining on the mail server for more than 60 days will be deleted. DSS e-mail servers do not keep copies of your e-mail after it has been delivered to your PC using MS Outlook. If you need to save e-mail, use the Outlook folders or use the **Save As** command and save it to your hard drive. A common location is in a subdirectory under **My Documents**.
- Size Limit. E-mail attachments are limited to 3 megabytes. Attachments greater than 3 megabytes will not be delivered.
- Stationery on E-Mail. Microsoft Outlook allows individuals to choose or create a background image on which e-mail text is placed. This stationery, while colorful and sometimes entertaining, places a significant burden on our e-mail servers, and should not be used on DSS' networks.
- Spam. Spam (unsolicited e-mail), junk mail and chain letter should not be created or sent by DSS employees and contractors. If you receive it, delete it. Don't pass it along.
- Suspicious E-mail. If you receive a suspicious e-mail, such as:
  - An e-mail that you were not expecting or from someone you haven't heard from in a long time,
  - An e-mail, which seems out of character or inappropriate to be coming from the sender (i.e., a "Love Letter" coming from a business associate, co-worker, etc.),

- An e-mail which has misspelled words, unusual sentence structure, all capital letters, etc., or
- An e-mail that has an attachment with a **vbs** extension (see Dangerous Attachments).

It is possible that the suspicious e-mail may contain a virus. If you cannot verify with the sender that the e-mail is legitimate and the attachment is safe, you should delete it without opening it.

- Viruses Protection Programs. E-mail is a common method for transmitting computer viruses and Trojan horses. For this reason it is important that your PC has an active virus protection program. At DSS we currently use **Symantec AntiVirus** software. Make sure that your **Virus Definition file** is up-to-date.

7.2.6 Victims of E-mail Abuse, Harassment or Threats

E-mail abuse, harassment and threats can and do happen in the workplace. If you are a victim of harassment from clients or other individuals, report the incident to your supervisor and the DIS Information Security Unit (email the Security Unit at sec900@email1.dss.state.va.us).

Please keep copies of the harassing e-mail messages, dates, and times of unauthorized access, etc., for investigative purposes. Each incident will be handled confidentially. DSS will protect the confidentiality of those involved to the extent permitted by law and to the extent that continued protection does not interfere with the DSS' ability to investigate allegations and to take corrective action.

Important: **Under no circumstances should you reply to abusive or threatening e-mails**.

7.3 Internet

7.3.1 Policy

Internet access introduces significant security exposures to DSS's computer equipment, systems and networks. This section, along with the policies and guidelines found in section 7.1 Network Security Overview, gives the minimum controls required to use the Internet safely from DSS.

7.3.2 Background

Department staff are encouraged to use the Internet to further DSS's mission; provide effective services of the highest quality to our customers; discover innovative and creative ways to use resources and improve our services and promote staff development. However, individuals need to remember that:

- Internet access opens an information conduit by which sensitive, and potentially private, information could be released onto the open network and the world.

- The Internet is not a secure environment and individuals should assume that whatever they are doing is being monitored both internally as well as by individuals interested in compromising DSS.

7.3.3 Requirements and Guidelines

Individuals must comply with all stated policies and will be held accountable for their activities.

- Downloading Data. Software or files downloaded from Internet into DSS's network becomes DSS property. Also DSS does not permit the downloading of the following:
  - Personal software, images, audio or videos;
  - Spyware, such as Bonzi Buddy, Comet Cursor, Gator, Hotbar, Morpheus, etc., collects and reports information about your system and your web surfing activities to marketing companies;
  - Entertainment software, games or playing games on the Internet;
  - Streaming audio or video files; or
  - Downloading or distributing pirated software or data.
- Encryption. Information pertaining to the department, its clients, and others who do business with DSS may not be transmitted over the Internet unless it is encrypted using department-sponsored encryption software. Confidential data transmitted across the Internet must be encrypted or transferred using an encrypted or secured session.

- Internet Use – DSS. Department and agency staff may use the Internet for direct job-related purposes, professional contacts and career development activities.
- Internet Use – Personal. Incidental personal use of the Internet is allowed provided that it is not excessive, it does not interfere with your job functions or the job functions of others, and it does not place an undo burden to the network. Please check with your manager for local policies that may place greater restrictions on Internet use.
- Large File Transfers. Due to the burden placed on the network, file size is limited to 3 megabytes. Also to lessen the impact of the file transfers, try to schedule transfers for off-peak times.
- Malicious Acts. Individuals are prohibited from using DSS' computers, systems and/or networks (including Internet access) to commit malicious acts. Please refer back to section 7.1.3 for additional information.
- Monitoring. As mentioned earlier in this section, when you use any of DSS' network services, you should have no expectation of privacy. DSS has systems in place that monitor Internet usage. These systems track items such:
  - Who you are
  - What sites you have visited
  - How long you were at the site
- News Groups, Chat Groups and Forums. Individuals are permitted to participate in various news groups, chat groups and forums (*Internet groups*). These groups are good sources of information and exchange of ideas. However, it is important to note that **all communications that leave your PC are traceable to the Virginia Department of Social Services, and to you, even if you use a pseudonym.** As a result, when you participate in *Internet groups*, you must adhere to the following guidelines:
  - When participating in *Internet groups*, all department policies apply (including but not limited to confidentiality, privacy, sexual harassment and the protection of intellectual property);
  - You must clearly identify yourself;
  - You should conduct yourself professionally and honestly, using the same standards and ethics as you would in the office;
  - Only authorized individuals may represent DSS in *Internet groups*;
  - Never disclose confidential information in *Internet groups*; and
  - You will be held accountable for violations of security, confidentiality or other provisions of the Information Security Policy when participating in *Internet groups*.

- Personal Internet Service Providers (ISP). Using your personal ISP (e.g. Erols, AOL, Hotmail, Excitemail, etc.) on a state owned PC does not release you from any of the provisions of these guidelines.
- Restricted Sites. Individuals are prohibited from visiting sites, which are restricted by the Code of Virginia, Chapter 52. Below is an excerpt from Chapter 52, the entire code is in Appendix B.

  RESTRICTIONS ON STATE EMPLOYEE ACCESS TO INFORMATION INFRASTRUCTURE.

  § 2.1-805. Restriction on agency employee access via computers to materials with sexually explicit content.

  "...no agency employee shall utilize agency-owned or agency-leased computer equipment to access, download, print or store any information infrastructure files or services having sexually explicit content."

  In addition to sites with a sexual content, hate sites and sites that use offensive language (i.e., profanity) are prohibited.
- Screen Savers. Personal screen savers are not permitted on State owned PCs. Only screens savers supplied with the computer's operating system are approved for use.
- Web Blocking. DSS uses web-blocking software to prevent access to undesirable sites.

7.4 Intranet (Network 2000)

7.4.1 Policy

To ensure the security and integrity of Network 2000, adequate system controls must be implemented and functioning.

7.4.2 Background

The department sponsors an Intranet, known as Network 2000, which connects the central, regional and district offices and local agencies together. This Intranet is the primary vehicle through which department information and system resources are shared. Network 2000 is a controlled and secured intranet, where as the Internet is open, uncontrolled and not secure.

7.4.3 Requirements

A department network administrator and backup administrator, whose primary responsibility is to coordinate and manage network activities must be appointed.

- Software. The network administrator must approve all software before being loaded into any of the department's file servers. Program files (e.g. .exe, .dll, .bat, and any other executable files) are not to be written to any network drives unless authorized in writing by the network administrator.
- Virus Scanning. All programs and data must be scanned by the department's anti-virus software before being introduced into the network.
- Backups. File servers shall be backed up on a frequency sufficient to permit timely recovery and minimal disruption. Weekly, full backups must be performed for each file server. On a daily basis, incremental backups should be performed.
- Off-site Storage. All backups must be stored off-site to ensure safety of the media.

7.4.4 *Localagency* Website

One of the services maintained as part of Network 2000 is the internal DSS website. This supplies DSS employees with current information about the agency. Some of the information found at this site includes:

- Local Agency Broadcasts
- A list of Local Division websites
- DSS e-mail directory
- Support Information Sites
- The DSS Functional Directory

Most DSS PC web browsers, such as Internet Explorer and Netscape, are set up to automatically go to this web page. It can also be reached using http://www.localagency.dss.state.va.us/ .

7.4.5 DSS Security Web Page

The DSS Security Web Page can be found under the *Localagency* Website. It is maintained by the DSS Information Security Unit to promote security awareness. The web page is located at http://www.localagency.dss.state.va.us/divisions/dis/is/index.html and you will find the following information:

- Latest security news.
- Security Newsletter, which covers security topics
- The names and contact information for the security staff

7.4.6 LAN Drives "H" and "W"

Central Office staff have access to network drives for storing and sharing information. The drive names will vary slightly base on your system name but will be similar to these examples:

Drive "H"	**JOM900 on 'DSSNAS1' (H:)**
Drive "W"	**CENTRAL on 'DSSNAS1' (W:)**

These network drives offer you some advantage over using your local hard drive on your PC.

- You can use these drives to store your files, giving you more storage capacity.
- Files stored on the network drives will be routinely backed up for you.
- Files can be saved on the network drives so the multiple individuals can access and share information.
- When you have a file greater than 3 megabytes (which is too large to be sent over the network) it can be exchanged using the network drives.

7.5 Remote Access

7.5.1 Policy

Remote access is limited to DSS state staff who, by the nature of their job, are required to work remotely from home or while traveling.

7.5.2 Requirements and Guidelines

Dial-up access via a modem poses a high risk of possible intrusion to the DSS network. It offers another avenue of access to DSS computers, systems and files. But there are times when the risk is offset by convenience and need. However, only DSS state employees are allowed to access DSS computer resources from offsite locations. A copy of the *Remote Network Access Request* form can be found in Appendix B.

Even though dial-up connections have risks, they are more secure than normal sessions established using the Internet. When using the Internet, there can be no presumption of confidentiality or security unless your session is encrypted or secure. Never access DSS systems over the Internet using a DSS assigned userID with a password in *clear text*. [1]

7.6 Modem Usage

7.6.1 Policy

PCs should not be connected to the DSS network while using a modem to connect to a remote site. Using dial up modems to access a remote host while the PC is connected to Network 2000 is strictly forbidden. Using dial up modems for non-department related business is not permitted. Using a remote access program (e.g., pcAnywhere) to access a PC connected to Network 2000 is forbidden.

7.6.2 Background

Crackers and hackers are always looking for a way to gain access to public or private networks. One way hackers can gain access to a private network is through a PC using a modem. If a PC has both a network connection (to a private network) and a dial up connection (using a modem to connect to a remote site), the PC can become a pass-through for a hacker. Using this technique, the hacker can bypass firewalls and system security, and have direct access to the private network. In DSS' case this would give hackers direct access to Network 2000.

7.6.3 Requirements

When using a modem to establish a dial up access for legitimate department business, the procedures below should be followed to minimize the risk to Network 2000:

a. Before making the dial up connection, close out all applications and physically disconnect the computer's network cable; (i.e. unplug your Ethernet cable). This will prevent someone from acquiring access to Network 2000 while you are using the dial up connection.

b. Connect your modem to the phone line.

c. Conduct your dial-up session.

d. Immediately terminate the dial up session as soon as you have finished your access. This will limit the amount of time someone can introduce an unauthorized program or transaction onto your computer.

e. Remove the phone line from your modem.

f. Reconnect your network cable.

g. Re-boot your PC as needed to re-establish local area network connections.

Section 8 – Viruses and Hoaxes

Computer viruses and other malicious codes create significant costs to business and government. These costs include staff time, system outages, and preventive measures. In this section we will list the types of malicious codes, discuss how you will receive virus alerts, explain the department's policy on anti-virus software and discuss computer hoaxes and chain letters.

8.1 Viruses and Malicious Codes

8.1.1 Policy

Individuals using DSS systems, computers, software and data will not knowingly create and/or distribute computer viruses or other malicious codes. In addition, individuals must never intentionally load and/or infect any system or computer with a computer virus or other type of malicious code.

8.1.2 Background

Viruses are one of several classes of malicious code. Also included in this group are *Macro Viruses*, *Worms*, *Trojan Horse* and *Network Worms.* The following will explain the characteristics for each class of malicious code:

- Trojan Horse. Named after the Greek myth of the Trojan horse. This program performs a useful function, but also performs an unexpected action that is usually malicious.
- Virus. A virus is a program segment which reproduces by modifying other programs to include a copy of itself.
- Macro Virus. This virus type spreads by documents created within an application. Microsoft Word and Microsoft Excel are frequently used to spread macro viruses.
- Worm. A worm is a program which replicates itself and causes execution of the new copy. [2]
- Network Worm. This is a worm that copies itself to another system by using common network facilities, and causes execution of the copy on that system. [2]

8.2 Virus Alerts

8.2.1 Policy

When DSS systems are threatened by a computer virus or another type of malicious code, the manager of the DSS Information Security Unit will issue an alert.

8.2.2 Background

When a malicious code is threatening our networks and computers, it is important to convey clear and concise instructions. If multiple and possibly conflicting instructions are sent from several sources, this may create confusion and delay efforts in containing the virus threat.

8.2.3 Requirements and Guidelines

When a virus threat exists that may impact you, the DSS Information Security manager will send a *Virus Alert* to all DSS employees and contractors. This alert will be sent out in at least one of the following fashions:

- A broadcast on the *Localagency* website,
- A mass e-mailing, or
- Prominently posted notices in the lobbies and entrances.

When you receive an alert you will be given a description of the threat, methods for identifying the threat, and special procedures to follow. Sometimes you will also be given information describing the actions to be taken if you are infected, and who to contact for help.

8.2.4 Reporting Viruses

If you receive information regarding a virus threat (usually e-mail), you should forward the information to your security officer, who will in turn forward the information to the DSS Information Security Unit. The Information Security Unit will investigate the information and if the threat is real, they will issue a *Virus Alert*.

Important: You should not send virus threat information to others, even if instructed to do so in the message. In a majority of cases, virus information received through e-mail is nothing more than a hoax. See section 8.4 for more information on hoaxes.

8.3 Anti-virus Software

8.3.1 Policy

Anti-virus software must be installed and must be operational on all personal computers and servers that access DSS information or information processing systems.

8.3.2 Background

The availability of and access to departmental information is paramount to the successful completion of the DSS mission. PC viruses threaten the availability of and access to this information. Viruses are proliferating at a staggering rate and the potential for infection increases daily. Everyone must do their part to ensure that department information processing systems remain virus free at all times.

8.3.3 Requirements and Guidelines

All personal computers and servers that access DSS information or information processing systems must have a current version of the department's standard anti-virus software installed and it must be operational. Additionally, the *virus definition file* must be updated daily and the hard drive must be scanned weekly for viruses.

8.3.4 Software

DSS' current standard for anti-virus software is Symantec AntiVirus Corporate Edition. This software has been install on most machines and must be active. A few local governments may require that McAfee AntiVirus software be used. This is permitted but the DSS Security Unit must be notified in writing and the local agency is responsible for keeping their virus definition files up to date. Symantec AntiVirus is the only virus protection software supported by DSS. This software is provided without charge to everyone who uses DSS systems.

The following is a discussion of some important features found on Symantec AntiVirus software. In most cases you will find similar features in other well-known anti-virus programs.

- *LiveUpdate*. This Symantec AntiVirus feature updates the *virus definitions files* automatically**.** *LiveUpdate* should be configured to automatically retrieve *virus definitions files* daily.

  This feature runs in the background and will have little or no impact on your PC's performance. The best time for *LiveUpdate* to run is when you begin your workday.

- *Schedule Scan*. Another feature of Symantec AntiVirus is the ability to schedule regular scans of your hard drive. This feature is found under the "*Schedule Scan*" option in Symantec, and should be set to run weekly.

  Scanning your hard drive will impact your PC's performance and you may want to schedule the scan to occur during your lunchtime. Important, do not schedule your scans for nights and weekends. Symantec AntiVirus Software cannot operate when your PC is turned off. Select a time during normal business hours to scan your PC.

8.4 Hoaxes and Chain Letters

8.4.1 Policy

Individuals using DSS computers, systems, programs and data should not initiate or forward computer hoaxes or chain letters.

8.4.2 Background

A hoax is a phony e-mail message warning you of a fake virus. It is intended to alarm you and overload computer networks because you are directed to send the alert to everyone you know. If you receive a hoax, don't pass it on.

8.4.3 Requirements and Guidelines

If you receive a virus warning and you are not sure if it is "real" or a "hoax" there are several steps you should take:

a. First check the Internet to see if the warning is listed as a hoax. You can look it up at the site listed below:

http://www.symantec.com/avcenter/hoax.html

If you determine that it is a hoax, don't pass it on. Simply delete it.

b. If you are still unable to determine if the warning is "real" or a "hoax", contact your security officer. Your Security officer can check his/her sources or will contact the DSS Information Security Unit to determine if it is legitimate.

c. Your security officer will let you know if the warning is "real" or a "hoax". As in step "a", if it is a hoax, simply delete it.

d. If it turns out to be an actual virus, DO NOT send out a warning. This will only add additional traffic to the network and may cause confusion.

Your security officer will contact the DSS Information Security Unit. The DSS Security Unit will issue the virus warnings to DSS offices, agencies and divisions.

8.4.4 Characteristics of a hoax

The most likely way you will receive a hoax is through your e-mail. It will probably come from either a friend or acquaintance that you correspond with using e-mail. These hoaxes will have some of the following characteristics:

- Some, if not all, of the message will be upper case letters;
- The message may use excessive explanation points;

- The message is intended to scare. It will use phrases such as "very dangerous", "NO remedy", and "Erases everything";
- It will use recognized names to sound convincing and to establish credibility, e.g. "IBM announces", or "AOL states"; and
- The message will encourages mass distribution, e.g. "Pass this warning along to everyone in your address book". (This last point is a classic characteristic of a hoax or a chain letter.)

8.4.5 Hoax Examples

Each hoax will vary in what it says and how it is written. The following are examples of recent hoaxes:

- It Takes Guts to Say Jesus Hoax

  VIRUS WARNING !!!!!!!
  If you receive an email titled "It Takes Guts to Say 'Jesus'" DO NOT open it. It will erase everything on your hard drive. Forward this letter out to as many people as you can. This is a new, very malicious virus and not many people know about it. This information was announced yesterday morning from IBM; please share it with everyone that might access the internet. Once again, pass this along to EVERYONE in your address book so that this may be stopped.

- Wobbler Hoax

  VIRUS ALERT If you receive an email with a file called "California" do not open the file. The file contains the virus. This information was announced yesterday morning by IBM. The report says that "this is a very dangerous virus, much worse than "Melissa" and there is NO remedy for it at this time. Some very sick individual has succeeded in using the reformat function from Norton Utilities causing it to completely erase all documents on the hard drive. It has been designed to work with Netscape Navigator and Microsoft Internet Explorer. It destroys Macintosh and IBM compatible computers. This is a new, very malicious virus and not many people know about it at this time. Please pass this warning to everyone in your address book and share it with all your online friends asap so that the destruction it can cause may be minimized.

8.4.6 Chain Letters

Chain letters are e-mails sent to you with promises of wealth, well-being, spiritual uplifting, or requiring your help for some worthy cause. The chain letter may ask for money and/or may threaten you if you break the chain. But all chain letters share one characteristic, they will require that you forward the letter to other people (typically 5 to 20). Chain letters can be categorized as a hoax or a fraud, and if you receive one you should delete it. DO NOT forward it to others.

8.4.7 Chain Letter Examples

As with a hoax, a chain letter will vary in what it says and how it is written. The following are examples of recent chain letters:

- Abercrombie & Fitch Chain Letter

  Hello everyone! My name is Amber McClurkin. You have probably heard about the email from Gap offering free clothes to anyone who will forward the message on. Well, I am the founder of Abercrombie and Fitch, and I am willing to make a better deal with you. You will receive a twenty-five dollar gift certificate for every five people you forward this to. This is a sales promotion in order to get our name our name out to young people around the world. We believe this project can be a success, but only with your help. Thank you for your support !!

  Sincerely,
  Amber McClurkin
  Founder of Abercrombie and Fitch

- ATM Envelope Poisonings

  Subject: FW: Sick city we live in

  Very scary!

  Please read.....

  Whenever you go to an automatic teller machine to make deposits, make sure you don't lick the deposit envelopes. (spit on it) A customer died after licking an envelope at a teller machine at Yonge & Eglinton. According to the police, Dr. Elliot at the Women's college hospital found traces of cyanide in the lady's mouth and digestive system and police traced the fatal poison to the glue on the envelope she deposited that day. They then did an inspection of other envelopes from other teller machines in the area and found six more.

  The glue is described as colourless and odourless. They suspect some sickco is targeting this particular bank and has been putting the envelopes beside machines at different locations. A spokesperson from the bank said their hands are tied unless they take away the deposit function from all machines. So watch out, and please forward this message to the people you care about.....Thanks

  Kimberly Clarkson

  Crime unit, Department for Public Health
  563-9905

Section 9 – Issue Specific Policies

9.1 Authorized Use.

9.1.1 Policy

Management is responsible for authorizing individuals they supervise the authority to access information and information processing systems.

9.1.2 Background

Authority to access information and information processing systems must be evidenced. Properly completed and approved Computer System Access Request form serve as evidence that the individual has the authority to access specific information and information processing systems.

9.1.3 Requirements and Guidelines

Directors, manager and supervisors who are authorized to grant access to information and information processing systems must be identified to the unit's security officer.

The Computer System Access Request form (see Appendix B - Forms) must be completed and retained by the unit's security officer for each person requesting access to DSS Information Systems. If an individual's access needs change, new forms must be completed. Local Agencies may use their own forms provided they include similar individual, system and approval information.

The Information Security Access, Inspection & Monitoring Policy (ISAIMP), see Appendix B - Forms. (see Appendix B - Forms) must be completed for all persons using DSS related information or information processing systems.

9.2 Backing Up Information

9.2.1 Policy

Electronic information (data files) that is a part of a benefit, service delivery or financial management system should be backed up and stored off site on a frequency that would allow it to be readily recovered with the least amount of data re-keying.

9.2.2 Background

Disasters happen and they don't have to be in the category of fires, floods and tornados to cause a major disruption in our ability to get the job done. The accidental loss of information on personal computer and floppy disks (due to static discharge, power surge, etc.) is far more common than natural disasters. An effective backup system is one of the best ways of assuring the ability to recover after a disaster.

Note: Mainframe System backup requirements are discussed in Chapter 3 – DSS Technical Staff.

9.2.3 Requirements and Guidelines

Every individual using DSS computers and systems is encouraged to make backups of their individual data on a routine basis. The more important the information is to a priority function, the more frequently it should be backed up. By creating backups, you will be protected from loss of data due to equipment failure, accidental erasure or overwriting of data, and malicious acts that may delete or alter your information. The following are some general guidelines for backups:

- Information that would be costly, time consuming or impossible to reconstruct should be backed up frequently.

- A backup copy of important information should be routinely rotated off site. The person owning the information (or his/her supervisor) should determine the off site location.

- Backups should be retained until a newer backup renders the older backup obsolete.

9.2.4 Backup Alternatives

There are a number of methods that can be used for backing up your personal information. The following are two common methods of creating backups of your information:

- Local Backups. Backups may be done locally by writing your important files and programs to diskette, etc. When using this method it is advisable to store your diskettes away from your workstation.

- Network Backups. Another option, available to Central Office staff, is the use of network drives. If you save your files to drives "H" or "W", they will be automatically backed up for you and stored off-site. Please remember, if you

have information that is highly sensitive (i.e. adoption, child welfare, etc.), it should be encrypted before you save it to a network drive.

9.3 Computer Games

9.3.1 Policy

Computer games should not be played on state-owned computers. Computer games should not to be played on state-time.

9.3.2 Background

In memos from the Governor's Office and the Secretary of Health and Human Services, playing computer games on state-owned computers and/or on state time shall not be done.

9.3.4 Requirements and Guidelines

Same as Policy.

9.4 Encryption

9.4.1 Policy

When sending confidential or sensitive information pertaining to DSS, its clients and others who do business with DSS over the Internet, the information must be encrypted.

9.4.2 Background

Encryption is the process of character substitution or transposition in a sequence determined by an encryption formula. Readable text (*clear text*) is converted to unreadable text, called cipher text, based on a security key provided by the owner of the information. Anyone examining an encrypted file would see a string of unrelated characters or symbols. The encryption process can be reversed or decrypted only by someone who has the security key. [1] Below is an illustration of a phrase in a readable format and in an encrypted format:

Readable Text	Encrypted or Cipher Text
Confidential information should never be sent over the Internet!	Tz09jdvOmeFXklnN/biudE/F/Ha8g8VHMG HOfMlm/xX5u/2RXscBqt

9.4.3 Requirements and Guidelines

The need for encryption is determined by the sensitivity of the information and the method you chose to send the information to the receipient. When sending confidential or sensitive Information using e-mail or the Internet use the following as a guideline: [1]

- Any e-mail or document containing confidential or sensitive information pertaining to the DSS, its clients and others who do business with DSS, which is sent across the Internet, must be encrypted using department sponsored encryption software or transferred using a secure or encrypted session.
- When using Network 2000 for sending e-mail, it is not necessary to encrypt data. This is a secured private network controlled by DSS. Any address found in the DSS directory will remain within Network 2000.

9.5 Illegal Copying and Unauthorized Use of Copyright Works

9.5.1 Policy

The duplication of software, manuals, books or other materials in violation of copyright laws and vendor licensing agreements is strictly forbidden. Infractions of this policy may result in a Standards Of Conduct being issued as well as civil and criminal penalties.

9.5.2 Background

The unauthorized duplication of software, manuals and other materials is theft. These products reflect a substantial investment of time, talent and money by the developers. Unauthorized duplication deprives the developers of fair compensation.

9.5.3 Requirements and Guidelines

Violations of this policy must be reported to the appropriate division, office, or agency director and to the Division of Information System's Information Security Unit. Violations of state and local laws will be reported to the appropriate law enforcement authorities.

9.6 Information Processing Systems and Equipment

9.6.1 Policy

Information processing systems and equipment must be protected against unauthorized use, theft, vandalism, fire/smoke/water damage, misappropriation, misapplication, or other peril.

9.6.2 Background

Information processing systems and equipment are department assets. They must be afforded a level of security appropriate with their value and with the sensitivity of the information they can access.

9.6.3 Requirements and Guidelines

- Authorized Use. Only authorized personnel are permitted to use information processing systems and equipment.
- Protection. Computer equipment, software, and documentation should be located in areas which afford protection from disasters. They should also be in areas that have restricted access and can be monitored.
- Inventory. The CCU (Customer Care Unit) enters PC and PC equipment information into a centralized inventory database at time of purchase. On an annual basis, CCU will validate the accuracy of the inventory database by comparing it to a physical inventory done by a sampling of 10% of offices and divisions.

9.6.4 Portable/Laptop Computers

Portable computer equipment (i.e. laptop and notebook computers) should be locked up when not in use or cabled to the desk/work station.

9.6.5 Personal Use

DSS computers, systems, networks, and other equipment cannot be used for any activity other than agency-related business except as specifically detailed in this policy (e.g. incidental use as described within this policy or as granted by your supervisor). Other personal use is prohibited.

9.7 Passwords

9.7.1 Policy

Individual passwords must be used to control access to information processing systems.

9.7.2 Background

An effectively implemented passwords control system can limit access to information systems to authorized personnel. To be effective, the passwords should be changed frequently, they should not be shared or disclosed to others and they should not be easily guessed.

9.7.3 Requirements and Guidelines

Each individual granted authority to access information processing systems should be assigned a unique userID, which will require a password for access.

- Confidentiality. It is the responsibility of each individual to keep his or her password confidential. Immediately report any suspected compromise or unauthorized use to your password to the security officer.
- Use of Another Person's UserID and Password. No one shall knowingly use the userID and password of another person to gain access to programs or data except as specified below in Staff Use of Supervisor UserID and Password.
- Staff Use of Supervisor UserID and Password. A supervisor may grant permission for their staff to use the supervisor's UserID and password(s) during an absence. This permission is granted to allow staff to access the supervisor's e-mail and data from the supervisor's hard drives and network drives to allow day-to-day business to continue in their absence. Immediately upon returning, the supervisor should change their password(s). Under no circumstances, however, should a supervisor give out his or her password to mainframe systems such as ADAPT, OASIS, APECS, etc.
- Frequency of Change. Passwords should be changed monthly.
- Password Storage. Passwords should not be written or stored in a manner accessible to others. However, if you must write them down, keep the password on your person to avoid the risk of compromising it.

9.7.4 Password Characteristics

All passwords must meet the following characteristics unless restricted by the operating system:

- Passwords must be at least eight characters long
- Passwords will contain a combination of:
    1. Upper case letters
    2. Lower case letters
    3. Numeric values

- The first character of the password must be a letter

9.7.5 Password Selection

When choosing a password it is important that you choose one that you can remember but would be difficult for others to guess. Below are some suggestions for choosing a password.

- Try combinations like you see on vanity license plates – M8kadeel (*Make a deal*)
- Put two short words together with a number – dent6raKe (*dent + 6 + raKe*)
- Use letters from a phrase or lyric with numbers – rmPi2h4m (*remembering my Password is 2 hard 4 me*)

9.7.6 Passwords to Avoid

- Avoid passwords that can be found in the dictionary; they are easy to crack with password cracking software.
- The names of your family, friends, associates or pets.
- Passwords based on your license plate number, social security number, or phone number should not be used.
- Don't use passwords that are part of a series of repeating or sequential characters or numbers.

9.8 Personal Computer Based Systems

9.8.1 Policy

PC systems using customer information or producing information used in decision-making or financial/statistical reporting must be documented, tested and approved.

9.8.2 Background

More and more people are learning how to use PCs and discovering techniques to help them perform their every-day tasks more efficiently and effectively. As a result, it is common for information to be down-loaded from mainframe computers to a PC. Individuals use this information to develop spreadsheets and database applications to manipulate the information for various needed purposes. The department encourages its employees to be creative and seek better ways to

satisfy their information needs. There are however, documentation, testing and approval requirements that must be observed when an information user develops applications (spreadsheets, data bases, fourth generation languages, MAPPER, query language processors, report writers, etc.) that use customer information or produce information used in decision-making or financial/statistical reporting.

9.8.3 Requirements and Guidelines

Required documentation includes a description of the application to include its: author, purpose, inputs, outputs, processes, calculations, controls, security, interfaces with other systems/processes, execution instructions, run schedule, error/exception handling, intended user and information retention.

Documentation must be of sufficient detail to provide someone other than the developer enough information to maintain and run the application.

The accuracy of the application as to outputs, processes, calculations, controls, security, execution instructions, run schedule, and error/exception handling must be verified in writing by someone other than the developer.

Responsible management must review and approve the application prior to implementation.

9.9 Using Non-DSS Provided Software on DSS Computers

9.9.1 Policy

The Department of Social Services allows the use of Non-DSS Provided Software on DSS personal computers providing the software is used to perform agency business and has been approved in writing.

9.9.2 Requirements and Guidelines

Department of Social Services computers are set up with a standard software suite that addresses the needs of most users. If additional software needs to be installed to perform agency business (e.g. Thomas Brothers), it must meet the following requirements:

- The software must be used in accordance with copyright laws and the licensing agreement of the company that produced the software, i.e. software intended for use on a single computer, may not be installed on more than one computer at a time;
- There must be sufficient proof of ownership, including the possession of the original diskettes and software documentation provided by the vendor;

- The software must not impact the performance of DSS approved software or DSS hardware;
- The Non-DSS Provided Software must be approved for use in writing by the director using the Request to Use Non-DSS Provided Software on DSS Computers form; and
- Also approved in writing by the DSS Customer Care / Operations Manager.

This policy applies to commercially produced software, shareware, public domain software and freeware.

The installation of any software on the Department's Network is strictly forbidden unless authorized in writing by the Manager of the NetCentric Unit.

Note: Personal software or screen savers are no longer allowed on DSS computers.

9.10 Streaming Audio and Streaming Video

9.10.1 Policy

Downloading, viewing or listening to audio and video transmissions over the network (referred to as Streaming Audio and Streaming Video) is prohibited.

Note: *RealAudio* is an example of a program that uses streaming audio files.

9.10.2 Background

Streaming audio and streaming video is the transmission of audio and video signals over a data communications network. Typically, this is a one-way transmission from the source to the receiver, similar to a radio or television.

The most common application on this technology is listening to music on your computer. Because of the large amount of network resources that this requires, Streaming Audio and Video are not allow on DSS computers or networks.

9.11 Vendor Relationships

9.11.1 Policy

Vendor access to agency information is permitted when it is required to perform a project or task that is in the interest of DSS and adequate safeguards are in place (e.g. signing an ISAIMP agreement and receiving appropriate security training). Vendor access to information requires director approval in writing.

9.11.2 Background

Allowing access to agency information to anyone outside the Department of Social Services may be necessary at times but this access must be carefully considered. [1]

- Restricted Access. Access may be restricted to specific terminal locations and granted for a period of days, weeks, or months, and should automatically expire at the end of the period. Access should be restricted to specific IT data or resources. [1]
- Competitive Restrictions. It may be appropriate to restrict the vendor's competitive activities if such activities could take unfair advantage of disclosed information. [1]

Appendix A – Glossary

Access - The ability to view, change or communicate with a computer system. Access includes execution of programs, reading and writing to files and deleting files or data.

ADP - Automated Data Processing

Application Criticality. When discussing data sensitivity and protection, criticality is the criteria used to measure the length of time that DSS can continue to function without the application.

Application Sensitivity. When discussing data sensitivity and protection, the sensitivity of an application is used to quantify the application's impact on DSS' mission, reputation, interest, assets, or resources if they were not available. It is determined by adding the application's criticality and confidentiality scores together and using the combined scores to categorize each application as having a high, medium or low impact if unavailable.

Authorized individual - Person granted the ability to access department information.

Backup - The copying of information to a medium from which it can be restored if the original is destroyed or damaged. Full backups copy all data in the system. Incremental backups copy only the information that has been changed since the last full backup.

Chain Letter - These are e-mails sent to you with promises of wealth, well-being, spiritual uplifting, or requiring your help for some worthy cause. The chain letter may ask for money and/or may threaten you if you break the chain. But all chain letters share one characteristic, they will require that you forward the letter to other people (typically 5 to 20). Chain letters can be categorized as a hoax or a fraud.

Confidentiality - Pertains to information that may only be disclosed to authorized individuals.

Contingency Management - Administration of a plan for responding to emergency situations. The plan includes performing backups., preparing critical facilities that can ensure continuity of operations in the event of an emergency. It is synonymous with disaster recovery plan.

Customer - Person requesting benefits and or services from the department.

Data Confidentiality. When discussing data sensitivity and protection, confidentiality considers the type(s) of data that is processed by the application and based on the data's required level of confidentiality, assigns a numeric score to the application.

E-mail or Electronic mail - Personal communications consisting of memos, letters, files, voice or video sent over computer networks. When public networks (e.g. The Internet) are used the sender has no control over message routing; therefore, Internet traffic is not secure. When private networks are used (e.g. DSS's Wide Area Network) the traffic is secure.

Guidelines - Statements or rules created to allow the development of local procedures to comply with this security policy.

Integrity - Ensuring information is changed only in a specified manner. Maintaining information in what is considered to be an accurate and correct format.

Internet - A loose confederation of autonomous networks distributed among military, academic, private and corporate sites that are interconnected via an open communications protocol known as TCP/IP. The Internet is a interconnected group of individual computers and networks around the world.

Intranet - Networks which utilize World-Wide Web technologies but which are limited to a single company or organization. Intranets are used to distribute information within an organization using resources developed for the Internet, but without the security concerns associated with Internet connectivity.

ISAIMP - Information Security Access, Inspection & Monitoring Policy. An agreement between the Department of Social Services and anyone who has access to DSS information or information processing systems, to maintain the confidentiality of DSS (and other agencies) information and to only use this information or system for authorized purposes.

LWA - Local Welfare Agency.

Network 2000 - The name of the Department of Social Services' Intranet. This network connects individuals in central, district and regional offices and local agencies together. This is a secure network. Messages transmitted through Network 2000 cannot be intercepted or attacked by individuals who are not permitted on the network.

Network Administrators. The technicians who design and operate computer system networks. They are responsible for implementing technical security on computer networks and for being familiar with security technology that relates to their network. They also ensure the continuity of their services to meet the needs of functional managers as well as analyzing technical vulnerabilities in their networks. [2]

Personal Software - Software not provided by the department, division, office or local agency.

Physical Security - Protection of computer systems and related buildings and equipment form fire, natural disaster, environmental hazards and intrusion. The use of locks, keys, and administrative measures to control access to computer systems and facilities.

Policy - A high-level plan identifying the department's philosophy regarding its information and information processing systems.

Public Domain Software - Software that is available free of charge to anyone. Registration is usually not required.

Requirements - Actions that must be included in the security procedures.

Resources - Items having operational, monetary or material value owned, leased or under care and custody of the department.

Sensitive Information - Information that, if lost or compromised would negatively effect the ability of the department to provide services and benefits to its customers (e.g. confidential information about recipients of DSS benefits or services). Also known as privileged.

Shareware. Software which may be copied and provided to anyone for evaluation purposes only. If the shareware is to be used, it must be must be registered and a fee paid to the developer in accordance with the licensing agreement.

Spyware. Spyware, sometimes referred to as "adware," is a hidden software program that gathers user information and transmits it to advertisers or other interested parties.

System Administrators. The technicians who design and operate computer systems. They are responsible for implementing technical security on computer systems and for being familiar with security technology that relates to their system. They also need to ensure the continuity of their services to meet the needs of functional managers as well as analyzing technical vulnerabilities in their systems and their security implications. [2]

Risk - The vulnerability of a particular threat to exploit an information resource's availability.

World-Wide Web (WWW) - A network of servers that uses hypertext links to find and access files on the Internet. Web browsers (e.g. Telnet, Gopher, etc.) allow you to view documents on servers around the world without having to know where the information is stored.

Appendix B – Forms

Most of the Security forms can be found on the Technology Business Support Services (TBSS) webpage, see link indicated below:

http://www.localagency.dss.state.va.us/tech_supp/ .

Some of the forms included are:

Exhibit 1 - Computer Access Request Form

Exhibit 2 - Information Security Access, Inspection & Monitoring Policy

Exhibit 3 - Request To Use Non VDSS Provided Software

Exhibit 4 - Remote Network Access Request Form

Appendix C – Security Policy Summary

http://www.localagency.dss.state.va.us/tech_supp/files/service_offerings/documents-manuals/VDSS_Information_Security_Policy_Summary.doc

Appendix D – References

1. Kansas Department of Administration Information Technology Security Policy, Developed by the DofA Security council, October 11, 1999.

2. NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook, Barbara Guttman and Edward A. Roback, October 1995.